METHOD FOR SECURELY CREATING AN ENDORSEMENT CERTIFICATE IN AN INSECURE ENVIRONMENT

RELATED APPLICATION

The present invention is related to the subject matter of the following commonly assigned, copending United States patent application: Serial No. 10/_____ (Docket No. RPS920030206US2) entitled "Method For Securely Creating An Endorsement Certificate Utilizing Signing Key Pairs" and filed December 31, 2003.

BACKGROUND OF THE INVENTION

1.   Technical Field:

[0001] The present invention relates generally to security features for computer systems and in particular to providing security features during manufacture and authentication of trusted platform modules (TPMs). Still more particularly, the present invention relates to a method and system for providing trustworthy endorsement certificates during manufacture of platforms using TPMs and the Endorsement Credential of that platform for that TPM.

2.   Description of the Related Art:

[0002] As the use of computers to conduct day-to-day business communication (information exchange) via computer networks increases, providing reliable/trustworthy encryption capabilities for each computer system has become a vital consideration in the manufacturing process for new systems. Even for computers utilized to carry out personal enterprises, such as Internet-based transactions, system (and network) security during these transactions is important.

[0003] One conventional method of providing security for information exchange via computer networks involves the utilization of certificate encryption. Certificate encryption involves the

utilization of public-private key cryptography (e.g., asymmetric cryptography). In order to provide this method of encryption, some sort of certification mechanism is required by which a certificate is provided by a trusted source to verify the trustworthiness of the encryption pair for a particular computer system. Those skilled in the computer arts are familiar with asymmetric cryptography and the implementation of public-private key pairs and associated certificate to carry out secure exchange of information between computer systems.

[0004] One major safeguard required during manufacture of computing devices that support certificate creation is against breaches in security (or inadequate security) that may result in the use of the private key being compromised. Such breaches may result in a fraudulent injection of an attacker's own public key to generate an endorsement certificate for a device not manufactured with the security safeguards required for a trusted source. An attacker inserts his own key into the process and obtain a certificate made for that key. Also, the endorsement certificate (digital signature) system is susceptible to fraud if the system using the high-value private key of a device is stolen, either by physical theft of the device containing the private key, or by discovery of the private key therein and subsequent copying and use in another device capable of generating endorsement certificates. Most importantly, one must protect the manufacturing environment such that the machine containing the high-value certification key can be assured it is only generating credentials or certificates for machines for which it should generate these credentials.

[0005] As will be appreciated, consumer trust is a key component of this system, and a manufacturer must ensure that there are no easy breaches to the system so that consumer trust can be maintained. Typically, users of a computer device are expected to rely upon blind trust in accepting that the device used to generate the certificate has not been stolen and in accepting that the device used to generate the certificate has sufficient safeguards to protect its private key from discovery and use.

[0006] With the need for reliable implementation of certificate creation within computer systems permeating the industry, the Trusted Platform Module (TPM) to implement the specification of the Trusted Computing Platform Group (TCG). The TPM is a chip that is manufactured to provide the encryption functionality in a trusted device, which is manufactured by a trusted

source. The specification of the TCG and TPM are available on the web at Internet address trustedcomputinggroup.org, and relevant content of that site is incorporated herein by reference.

[0007] A TPM vendor is required to implement a part that is complaint with the TCG main specification. An OEM of a system that has a TCG complaint part must go to further steps to create a Platform Credential that, in part, contains information about the Endorsement key in the TPM. The actual creation time of the Endorsement key is not important, but it is important that this key be created if a Platform Credential is to be created by the OEM. Since the platform is only in a controlled environment up until it leaves its manufacturing facility, this is when the credential should be created so that the OEM has a level of assurance that any credential it is signing is indeed for a platform created within its secured environment.

[0008] The Endorsement key created is a public/private key pair generated internally to a TPM. The public portion is the portion that is signed by the platform manufacturer. The use of this key is further explained in the TCG main specification. Since the OEM must feel assured that it is signing EK public keys from systems that it created, one may envision that a manufacturing facility would have a central machine with a high-value key that creates credentials for all machines within the secure manufacturing facility. However, it is not always feasible to have localized, high-performance cryptographic devices with high-value keys in the same manufacturing environment. Also, there is still no assurance that some attacker has not placed a rogue machine or even just a rogue key request in the facility to be signed.

[0009] The manufacturer of the TPM signs a certificate that is physically associated with the TPM. This certificate is tied to the public portion of the endorsement key, and together they confirm that the public key is the endorsement key of this particular TPM. The certificate generation mechanism is require to show public certification of the keys so the users can feel confident that the systems are indeed secure. Thus, there is great value in having the certificate that says that the public key was generated inside of a TPM.

[0010] Previously, manufacturers were able to protect their device manufacturing process by manufacturing the devices in OEM owned and operated manufacturing facilities that were safeguarded against external attacks. The devices were thus manufactured in a secure environment (i.e., an environment having a sufficient security rating so as not to compromise the

security level of any device manufactured in the environment and one from which an endorsement key could be trusted).

[0011] Typically, the manufacturing facility and the secure database (server) are not located at the same physical location, and the former is provided a much less secure environment than the latter. Also, while some OEMs own and control the manufacturing plants in these other locations, others license out the manufacture of the devices to a manufacturing vendor. These vendors often do not have the same sense of urgency or financial ability to provide adequate security against breaches/attacks in the manufacturing process.

[0012] With the globalization of the manufacturing workforce, due to economic and other considerations, many companies are now establishing/utilizing manufacturing plants in other locations outside of their direct control and trusted security environment (e.g., countries with cheaper labor). While steps are taken to provide security to these plants and limit their exposure to breaches or attacks, etc. in the manufacturing process, it is more likely and certainly not uncommon for security features of a remote facility to be compromised.

[0013] The OEM must protect the key in order to provide a credential for all customers by signing the keys. One method of protecting the key generation process involves placement of very expensive hardware (i.e., an credential server) at each remote manufacturing plant. However, obvious problems with this method includes: (1) controlling security of the "trusted" sever would become even more difficult when the hardware is placed in such a remote location; and (2) even if security could be guaranteed, the expense of providing such high-end secure systems for each manufacturing facility is very impractical (i.e., to expensive to implement).

[0014] Conventional credential servers located within the OEM environment must be able to determine/ascertain which keys to sign and which ones not to sign. For example, with 1000 devices in a manufacturing line, the credential server has to sign the endorsement keys being returned to each machine. The credential server needs to know each device from which the server receives a public key is a device that should be provided an EK certification. With no way to ascertain whether the keys were generated within the TPM, the credential server has no way of making this confirmation. Providing an endorsement certificate to even one EK not

generated within a TPM of the manufacturer could severely compromise the trust placed in the OEM by the customers who ultimately utilize the devices.

[0015] Thus, current manufacturing environments at which TPMs request a certificate from a remotely located trusted source are susceptible to security problems. The lack of security or inadequate security provides little comfort to the OEM that a certificate should be issued for all requests without having to consider the possibility that the process has been tampered with or that private keys have been generated outside of the TPM. A method and system that provides some additional confirmation that an authentication certificate is validly issued to an endorsement key from a key pair generated within a TPM would be a welcomed improvement to the manufacturing process.

SUMMARY OF THE INVENTION

[0016] Disclosed is a method and system for ensuring security-compliant creation and signing of endorsement keys of TPMs manufactured in a second party manufacturing facility. The endorsement keys are created as a pair of asymmetric keys with a public key and a private key. These keys are generated by the TPM vendor/manufacturer according to the TCG protocol. Prior to generating the devices, the TPM manufacturer selects an N-byte secret and stores the N-byte secret into the TPM. The N-byte secret is generated for every X machines, where X is a small enough number to discourage an attacker attempting to figure out the secret number while the devices are being manufactured an authenticated and X is large enough to substantially minimize the cost of having to inject a new N-byte secret number every X devices.

[0017] With an X value of 1000, for example, each batch of 1000 machines has the same secret, and the next batch of 1000 has a different secret. The secret is placed inside of the TPM and cannot be read outside of the TPM. Also, the secret is used once by the TPM, is never readable outside the TPM, and is destroyed after it is used.

[0018] In an alternate embodiment, X is a time factor and represents the number of devices that can be generated within X time. The time value is selected based on the same two above criteria for the numeric value selection. Thus, with an X value of 6 hours, assuming 1500 devices are manufactured every 6 hours, then each of those 1500 devices share the same secret number while the next 1500 devices share a different secret number.

[0019] The secret number is also provided to the OEM prior to the manufacture of the devices. During creation of the endorsement key, the TPM returns the public endorsement key as well as the necessary request digest. This digest is a one-way hash of the public endorsement key and the N-byte secret known only to the TPM and the OEM. The N-byte secret is destroyed once the hash value of the endorsement key is generated. This prevents an attacker from being able to crack the number. If the TPM is using one of the secrets previously provided to the credential server, the credential server matches the hash within the endorsement key with a second hash of the received public key (from the endorsement key) with the known secret number. Once a match is confirmed, the credential server generates the certificate. In one embodiment, the

ability of a TPM to utilize a hash value containing the secret number is valid for a pre-established time and expires after a passage of that time.

[0020] The above as well as additional objects, features, and advantages of the present invention will become apparent in the following detailed written description.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] The novel features believed characteristic of the invention are set forth in the appended claims. The invention itself however, as well as a preferred mode of use, further objects and advantages thereof, will best be understood by reference to the following detailed description of an illustrative embodiment when read in conjunction with the accompanying drawings, wherein:

[0022] **Figure 1** is a system diagram depicting a TPM manufacturing plant, customer device, and central certificate server, which collectively provide the environment within which the certificate authentication process of the present invention is completed;

[0023] **Figure 2** is a block diagram of a customer computer system with a TPM chip according to one embodiment of the invention;

[0024] **Figure 3** is a block diagram of an exemplary TPM platform within which various implementation steps of the invention are practiced, according to one embodiment of the invention;

[0025] **Figure 4** is a flow chart illustrating the method of providing certificate endorsement for a TPM's endorsement key using hashed secret numbers in accordance with one embodiment of the invention;

[0026] **Figure 5** is a flow chart illustrating a customer push of the certification process according to one implementation of the present invention.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENT(S)

[0027] The present invention provides a method and system for verifying that an endorsement key was generated within a TPM before creating an endorsement certificate for the TPM device. The invention eliminates the problems inherent when TPMs are being manufactured in environments that are susceptible to attacks. The invention is described from the perspective of a remote manufacturing environment (i.e., one that is geographically remote from the OEM's credential server). However, the features of the invention may be applicable to all manufacturing environments including those local to the credential server (i.e., one that is owned and controlled by the OEM). The TPMs are manufactured with standard private-public key pairs that require endorsement certificates from a trusted source (per TCG specification, which has been previously incorporated by reference.)

[0028] The invention describes a credential server of the OEM as the trusted source. Implementation of the invention requires some hardware/software overhead in both the TPM and the credential server, as well as some additions to the manufacturing process. As described, the hardware/software overhead includes a register comprised of a selected number of bits and, in one embodiment, logic for hashing the value within the register with the public key of the key pair.

[0029] The invention is best understood with reference to the various figures of which **Figure 1** provides a general overview of the manufacturing and authentication environments (or systems), within which the features of the invention are implemented. As provided by **Figure 1**, remote manufacturing plant **103** includes a computer **104**, which is utilized during the manufacturing process to complete several controllable (programmable) processes, such as injecting a selected/generated endorsement key pair and secret number (hereinafter "secret") into the TPMs. Manufacturing plant **103** manufactures customer devices (or platforms) **101** that include a TPM chip created for an original equipment manufacturer (OEM). The OEM environment **108** includes a credential server **107** with a high security value. Credential server **107** comprises a high-end processing component and affiliated database **106**, within which is stored a record of issued endorsement certificates and secrets received from the manufacturing plant's computer **104** (or personnel) via some secure transfer.

[0030] Remote manufacturing plant **103** is communicatively connected to credential server **107** via network **105**, which may be a WAN or LAN depending on the remoteness of the remote manufacturing plant **103** from the OEM environment **108** and the level of network security desired. Network **105** may be utilized to pass secure information between remote manufacturing plant **103** and credential server **107**. As will be described in greater details below, customer device **101** comprises a TPM **150** which issues an endorsement key request **110** for an endorsement certificate to credential server **107** and, in return, receives an endorsement certificate **112** from credential server **107** during the authentication process.

[0031] Both credential server **107** (within OEM environment **108**) and remote manufacturing plant **103** have some level of security, indicated by security columns to the right of each block. Credential server **107** is maintained with maximum security, while remote manufacturing plant **103** has some security value between minimum and maximum security levels. The invention assumes that the level of security at credential server **107** is necessarily at a highest level, while that of remote plant is not necessarily so. The invention operates within that overall system environment to allow a less than completely secure manufacturing facility to still be provided endorsement certificates for the manufactured TPM key pairs.

[0032] **Figure 2** illustrates an exemplary customer device or platform, which represents any one of a number of different devices that may comprise a Trusted Platform Module (TPM), designed according to the Trusted Computing Group (TCG) protocols. Specifically, device **101** comprises a processor **210**, a memory controller **220**, a system memory **230**, an input/output (I/O) controller **240**, and an integrated circuit (IC) device (i.e., TPM) **150**.

[0033] The I/O controller **240** performs I/O functions and supports communications with the TPM **150** via link **160**. Also, the I/O controller **240** supports communications with components coupled to other links such as a Peripheral Component Interconnect (PCI) bus, an Industry Standard Architecture (ISA) bus, a Universal Serial Bus (USB), a Firmware Hub bus, or any other bus configured with a different architecture than those briefly mentioned. I/O controller **240** may provide the connection means for linking computer system to network and ultimately to credential server.

[0034] **Figure 3** provides an exemplary embodiment of the TPM **150** of **Figures 1 and 2**. TPM **150** comprises one or more integrated circuits placed within a protective package. As further shown in **Figure 3**, TPM **150** comprises an input/output (I/O) interface **310**, a processor **320**, internal memory **330** (e.g., volatile and/or non-volatile), an asymmetric key generation unit **340** and a cryptographic engine **350**. Depending on implementation, the cryptographic engine **350** may be part of the processor **320** or separate logic/component.

[0035] The asymmetric key generation unit **340** is configured to create one (or more) asymmetric key pairs, which includes an asymmetric private key **361** and a corresponding asymmetric public key **362**. Each asymmetric key pair is used for encryption and decryption operations during a single communication session with another platform and may be erased after completion of the communication session either automatically or through issuance of an authenticated software command. The generated keys are stored within memory **330**. Also provided and stored within memory **330** is a secret **363**, which, as is further described below, enables a secondary security check by which the EK certificate may be provided with knowledge that the TPM private key **361** was generated within the TPM **150**. At some stage of the authentication process, the endorsement key certificate may also be stored within the memory **330** of TPM **150**.

[0036] TPM **150** allows access to certain entities stored in a portion of the internal memory **330** and/or performance of selected operations by its platform only upon receipt of authorization data (e.g., endorsement certificate) by the processor **320**. In order to protect the confidentiality of an authorization secret (and endorsement certificate) during transmission to the TPM **150** as well as insure the integrity of the endorsement certificate, the TPM **150** utilizes a secure data transmission mechanism. The confidentiality of transmissions is protected through encryption of the endorsement certificate. Likewise, the certificate's integrity is protected by the ability of the credential server to verify that the endorsement certificate is being transferred to a TPM and that only a specific TPM can decrypt the data.

[0037] **Figure 4** illustrates a flow chart of the process completed in a first implementation of the invention. It is understood that the various steps are illustrated in a particular order simply for the present embodiment and other variations in the order of process steps (and processes with

additional or fewer steps covering the same general concepts) fall within the scope of the invention. At step **401** of the process, the manufacturer (TPM vendor) builds the TPM chip.

[0038] Prior to or concurrent with generating the devices, a TPM vendor generates an N-byte secret number that is periodically changed, as is provided by step **403**. The value of N is a parameter that is selected based on one or more of the following: (1) cost of implementation; (2) difficulty to crack by brute force attacks; (3) length of time during which the secret number is valid; and other factors. For illustrative purposes, N is assumed to be 20. The size of the register that has to be included within the TPM to hold this secret is proportional to the size of the secret, as is the amount of storage space required in the credential server's database. Also, the method of injecting the secret number into the TPM, and the amount of logic required to complete the hashing function (described below) are also determined by the value of N.

[0039] A period, X, is identified for changing the secret number. X may be calculated based on a number of chips manufactured (e.g., every 1000 chips), or based on a passage of time (e.g., every 5 days), or some other basis selected by the manufacturer (or the OEM). The N-byte secret is generated for every X machines, where X is a small enough number to discourage an attacker attempting to figure out the secret number while the devices are being manufactured an authenticated and X is large enough to substantially minimize the cost of having to inject a new N-byte secret number every X devices. With an X value of 1000, for example, each batch of 1000 machines has the same secret number, and the next batch of 100 has a different secret number.

[0040] In an alternate embodiment, X is a time factor and represents the number of devices that can be generated within X time. The time value is selected based on the same two above criteria for the numeric value selection. Thus, with an X value of 6 hours, assuming 1500 devices are manufactured every 6 hours, then each of those 1500 devices share the same secret number while the next 1500 devices share a different secret number.

[0041] Once the secret is generated, the TPM vendor provides the 20-byte number to the OEM, at step **405**. This transfer occurs in a secure exchange and at the time the number is generated, which may be some time before the secret is actually used. The OEM's credential server records the secret number for later use during an endorsement key credential process.

[0042] The public/private endorsement key pair is generated and stored in the TPM, as indicated at step 406. The vendor also injects the secret into the TPM as shown at block 407. The manufactured TPM chip thus comprises the public/private key pair and the secret stored in memory. As with standard key pairs, the public key is available for public display and is transmitted across the network during authentication. The private key is internal to the TPM and not accessible once generated. The secret is also not accessible outside of the TPM. According to the present embodiment, the secret is a single-use-only number. Thus, once utilized during the credential process, described below, the secret is destroyed/deleted.

[0043] After the TPM (chip and/or platform) has been fabricated, the credential process is initiated. The TPM chip is installed in the computer system at step 409 and provided a secure connection to the credential server. Then, at step 411, the TPM generates a public endorsement key (EK) utilized within the credential process. The generation of the EK may occur at/during manufacture of the TPM or at some later time in an environment in which the private key is protected (not revealed). According to the present embodiment, during creation of the endorsement key, the TPM returns the public endorsement key as well as the necessary request digest. In the present embodiment, the digest is a one-way hash of the public endorsement key and the N-byte secret known only to the TPM and the OEM. The combination of these values is hereinafter referred to collectively as the endorsement key (EK).

[0044] The N-byte secret is destroyed once the hash value of the endorsement key is generated as shown at step 413. This prevents unauthorized use of the number in a security attack on the TPM. Also, this necessitates a brute force attack of the secret number to be carried out across multiple TPMs, making it very unlikely for such an attack to be successful. Potential attackers are thus prevented from being able to crack the secret number.

[0045] Following generation of the EK, the EK (PuK and hashed value) is forwarded to the credential server of the OEM at step 415. As previously described, this credential server is located within a high-value security environment that is validated by the OEM.

[0046] In one embodiment, the credential server is an on-site, highly protected, FIPS-4, RSA engine (e.g., 4758 processor), which provides high-performance, very secure crypto processing. The RSA engine also knows the 20-byte secret number and any necessary revocation data about

the shared secret numbers. FIPS (or Federal Information Processing Standards) is known in the art and the specification may be found at Internet site csrc.nist.gov/publications/fips, relevant content of which is incorporated herein by reference.

[0047] At the credential server, an expected hash value is calculated using the secret provided beforehand by the TPM vendor and the public key portion of the EK, as depicted at step 416. A comparison is made of the EK hash value against the calculated hash, and this comparison leads to a determination at step 417 whether the EK's hash value matches the expected/calculated hash value. If the values do not match, then the public key cannot be authenticated as coming from a secure TPM and a failure to authenticate is signaled to the customer device as shown at block 423. This failure is also recorded along with identifying data of the customer device and the TPM vendor. This information is recorded in a "failed credential" database associated with the credential server and may be utilized to track attempts to crack the system from a particular manufacturing site (or TPM vendor).

[0048] When the EK is confirmed as originating from a secure TPM, an EK certificate is generated by the crypto engine of the credential server and sent back to the TPM, as shown at step 419. The EK certificate is then inserted into the TPM at step 421 to enable future authentication processes to be completed/authenticated. The endorsement certificate is public readable but once writeable, so that the device only needs to be certified once.

[0049] Figure 5 is a flow chart illustrating a second possible implementation of the invention (or simply a second embodiment for the previous implementation). As in the previous embodiment, the public key and the hashed value are sent to the OEM. The credential server receives the EK at step 501 and generates the EK certificate (following confirmation by the credential process) and stores the EK in a server database, as depicted at step 503. The customer is required to request the certificate from the OEM for this TPM at some later time.

[0050] The credential server monitors for a receipt of a request from the customer computer for the EK certificate and, at step 504, a determination is whether the customer has made a request for the EK certificate. When the customer has made a request for the EK certificate, the credential server forwards the EK certificate to the customer's TPM, as shown at step 505. Notably, in another embodiment, the public endorsement key serves as a trigger that is sent by

the customer at a later request time to initiate the credential process, which generates the certificate and immediately forwards the generated certificate to the requesting customer. The EK certificate is inserted within the TPM as indicated at step **507**, and encryption functionality of the device is enabled. Only an approved EK certificate, based on one of the above credential processes on a specific customer device, is provided in response to a request from that specific customer. As is indicated at step **509**, the TPM is not enabled with secure encryption functionality until the customer has requested and received the EK certificate.

[0051] By completing one of the two embodiments described above, a TPM manufactured at a remote location may be authenticated and provided an EK certificate from the trusted OEM. Both the OEM and users of the device are able to trust the validity of manufacturing and credential process and resulting EK certificate and private key irrespective of the location at which the device was manufactured.

[0052] It is important to note that while the present invention has been described in the context of a fully functional data processing system, those skilled in the art will appreciate that the mechanism of the present invention is capable of being distributed in the form of a computer readable medium of instructions in a variety of forms, and that the present invention applies equally, regardless of the particular type of signal bearing media utilized to actually carry out the distribution. Examples of computer readable media include: nonvolatile, hard-coded type media such as Read Only Memories (ROMs) or Erasable, Electrically Programmable Read Only Memories (EEPROMs), recordable type media such as floppy disks, hard disk drives and CD-ROMs, and transmission type media such as digital and analog communication links.

[0053] While the invention has been particularly shown and described with reference to a preferred embodiment, it will be understood by those skilled in the art that various changes in form and detail may be made therein without departing from the spirit and scope of the invention.